Terrorism Risk and the Transportation of Spent Nuclear Fuel and High Level Radioactive Waste

Prepared by

James David Ballard, Ph.D.

California State University, Northridge (CSUN)
Associate Professor, Department of Sociology
Director, CSUN Intelligence Community Center Academic Excellence (IC-CAE)
Consultant for Nevada's Nuclear Waste Project Office.

Contact information:
California State University, Northridge
18111 Nordhoff Street
Northridge, CA 91330-8318

Telephone: 818.677.2009
Facsimile: 818.677.2059
E-mail address: ballard@csun.edu

Testimony to:

United States Senate
Commerce, Science and Transportation Committee

September 2008

Prepared Statement of:
James David Ballard, Ph.D.
California State University, Northridge

United States Senate
Commerce, Science and Transportation Committee

Hearing on Safety and Security of Spent Nuclear Fuel Transportation.
Russell Senate Office Building, Room 253
September 24, 2008

INTRODUCTION

Mr. Chairman and distinguished members of the Committee, thank you for asking me to testify at these hearings. My name is Dr. James David Ballard and I am currently employed as an Associate Professor of Sociology at California State University, Northridge (CSUN).[1] As part of my academic appointment I am also the campus director for the ODNI funded Intelligence Community Center for Academic Excellence (IC-CAE) program.[2] In an effort towards full disclosure, you should also know that I have had an on-going relationship as a consultant to the state of Nevada Agency for Nuclear Projects (NANP) since 1995.[3]

Over the last fourteen years I have been privileged to specialize in studying issues associated with human initiated events, defined as terrorism, sabotage, etc that may transportation efforts for the proposed Yucca Mountain shipments of spent nuclear fuel (SNF) and high level radioactive wastes (HLRW). The statements made today reflect my own individual opinions and are not necessarily those of any of these institutions I am associated with, nor do my comments necessarily reflect the opinions of my co-authors on cited references herein.

The foundations of my testimony arise from fourteen years of study on the issues surrounding potential terrorist attacks against shipments. During that time I have been privileged to be part of several multi-disciplinary teams of researchers that have studied the risk of terrorism attacks on nuclear waste shipments to the proposed Yucca Mountain storage facility.[4] In particular, we as a body of scholars, study the changing nature of terrorism and the terrorist tactics that could be employed against radioactive waste shipments. As part of this on-going effort we have identified a range of risks associated with transportation of these materials. On two previous occasions I have testified before either the House or Senate on the issues we discuss today.[5]

I appreciate the opportunity to brief this body on our work regarding the potential of terrorism attacks against the shipments of spent nuclear fuel (SNF) and high-level radioactive wastes (HLRW) that may be sent to the proposed Yucca Mountain facility. I hope the following discussion will help you and the agencies involved in regulating the potential shipments to

better understand the value of a social scientific perspective on SNF transportation. I will begin by discussing an issue that has been neglected in the debates since it was introduced nearly ten years ago – the target rich environment that these shipments represent. Secondly, I will concentrating on several other pressing issues not yet addressed in any adequate form by the DOE relative to the Yucca Mountain project. Following this summary of issues, this testimony will offer a systematic risk assessment protocol that can help overcome some of the deficiencies that the DOE has in their DEIS, EIS and SEIS documents, one critical basis of their planning efforts to date on Yucca Mountain shipments. Lastly, this presentation will suggest several ways that you may wish to review the transportation planning from an alternative perspective than that presented by the DOE. These alternative issues are a way I believe you can gain insightful evidence into the terrorism related threats these shipments face.

TARGET RICH ENVIRONMENT

The DOE has for decades tried to find a way to manage the terrorism risks associated with the proposed Yucca Mountain project with little overall programmatic success. Over that extended timeframe the expenditures of rate payer and taxpayer funding for this agency and its efforts have produced some less than stellar social scientific results with respect to the risks of human initiated events. Make no mistake, what we take about when discussing the transport of SNF and HLRW shipments are potentially very dangerous cargos and highly symbolic targets. They are a danger to the transportation infrastructure, to the public health and to the long term economic viability of the location(s) where an accident and/or terrorist attack may transpire. This is a social fact, no matter the rhetoric used by the industry and/or DOE to obscure this reality. Listen carefully to what is said and ask yourselves if it designed to obscure the issues from law makers, the public and the many stakeholders who are concerned about the shipment campaign necessary to stock the proposed Yucca repository.

In contrast to the DOE and nuclear industry perspectives, what the critics say is typically designed to see any Yucca Mountain transportation program conducted in a manner consistent with NEPA requirements. That is, the suggestions made by these critics compel the DOE to follow the spirit and letter of this law when looking at the transportation planning for this particular large scale federal program.

One critical issue typically neglected by the DOE is the recognition of this shipment campaign as a danger to the public. In other words, any Yucca Mountain transportation program that becomes necessary to transport the nation's stockpiles of highly radioactive waste is a security risk in and of itself. What DOE seemingly fails to understand is that this large scale federal program will draw the attention of a wide variety of adversaries because of its symbolic value – briefly it is nuclear, it is federal and it is controversial. The choice of a geographic location far

distant from the production sites where SNF and HLRW are generated assists the adversaries since it:

- Necessitates the movement of large numbers of shipments.
- Allows for the adversary to chart movement of these shipments in a predictable way.
- Is exacerbated by choices the DOE makes. For example, decisions that allow for hotter fuel, thus higher potential harm, to be sent along these predictable corridors.
- Will entail lengthy shipment routes that average over 2000 miles of open, unprotected terrain where an adversary can pick and choose the attack site.

Collectively these and other avoidable/manageable risks can be discussed as constituting a target rich environment.[6] The idea of a target rich environment is derived from military parlance. In this case we should consider:

- The totality of the shipment routes as the battle space.
- The attackers as potential adversaries with their choice of weapons and tactics.
- The shipments themselves as poorly defended, high value, symbolic targets.
- The perpetration of an attack against these shipments being a highly symbolic statement by the adversaries.

Under this definitional schema the DOE's transportation choices become increasingly important. This issue alone may suggest that sheltering the wastes in place,[7] at their point of origin, may be a more optimal safety and security strategy since the highly radioactive wastes will be protected from entering the target rich environmental battle space. The next section of this testimony reviews ten more critical issues that should prompt reconsideration by this body when deliberating the logic of the Yucca Mountain project and its potential to present a target rich environment to adversaries, both foreign and domestic.

PRESSING ISSUES

Recently Nevada summarized a top ten list of issues of concern during a presentation at the foremost nuclear industry conference, Waste Management 2008.[8] Since enactment of the NWPAA, and adoption of Assembly Concurrent Resolution 8 by the Nevada Legislature in 1987, NANP has consistently made recommendations to DOE regarding transportation safety and security, including many in this listing. The top ten measures are summarized in Table 1.

Figure 1: Ten Issues of Concern[9]

1. **Ship the oldest fuel first.**
2. **Shipments should be mostly rail, but truck shipments are necessary to complete the task.**
3. **Use dual-purpose casks.**
4. **Use dedicated trains.**
5. **Conduct full-scale cask testing (regulatory & extra-regulatory).**
6. **Engage in a meaningful NEPA process for selection of rail spur.**
7. **Use the WEIB "straw man" routing process.**
8. **Start the sec 180(c) program rulemaking.**
9. **Allow for state regulatory enhancements (safety & perception).**
10. **Rethink assumptions about terrorism and sabotage concerns**

- **Ship the Oldest Fuel First.** Nevada has recommended that DOE ship the oldest SNF first. This recommendation is supported by NAS and GAO since they also recommend shipping older fuel first. For example, shipping SNF that has been "aged" 50 years out of reactor, compared to shipping 5-year-cooled SNF, could reduce radiological hazards significantly and assist in lowering the risks of human initiated events.
- **Shipments should be by Rail.** Nevada has recommended that DOE utilize rail as the preferred mode of transportation, while acknowledging the serious impediments to developing rail access to Yucca Mountain and from 24 of the 76 shipping sites. Based on shipping site current capabilities, the share of SNF that could realistically be shipped by rail may be 65-75 percent, not the ~90 percent projected by DOE. Thus, DOE must first admit to the realities of the proposed shipment campaign and start planning for large numbers of truck shipments under the "mostly rail" shipment scenario. This would then entail a serious reconsideration of the safety and security requirements necessary to protect shipments.
- **Use Dual-Purpose Casks.** Nevada has recommended that DOE base its transportation system on use of dual-purpose (transportable/storage) casks of a standardized design, with a range of capacities resulting in loaded cask weights of about 125, 100, and 70 tons. In 1995, Nevada endorsed a previous DOE transportation plan that would have used a multi-purpose canister (MPC) system for transport and storage. DOE's current proposal to use the proposed TAD (Transport, Aging and Disposal) canister system does not fully address this issue. This operational choice by the DOE may actually complicate and further constrain the transportation system.
- **Use Dedicated Trains.** Nevada has recommended that DOE use dedicated trains for all rail shipments. Until DOE commits to only use dedicated trains, DOE routing studies and risk analyses must evaluate use of both dedicated and general freight rail shipments.

This adds to the complexity of any analysis, but more importantly without the commitment of dedicated trains, the safety and security of shipments may be compromised. Securing SNF/HLRW shipments in general freight poses significant challenges and greatly increases the risk of terrorism or sabotage during transport.

- **Commit to Meaningful Cask Testing.** Nevada has recommended that DOE and/or NRC conduct a meaningful full scale cask testing program. DOE or NRC should conduct full-scale regulatory tests on each cask design (or in cases of similar designs, test one cask from each representative grouping). DOE or NRC should also conduct a combination of extra-regulatory, full-scale testing, scale model testing, component testing, and computer simulations to determine cask failure thresholds. In addition, DOE and/or NRC must ensure meaningful stakeholder participation in all aspects of the cask testing program. Lastly, DOE and/or NRC should also couple this testing with new insights into the potential for human initiated events like sabotage and terrorism (extra regulatory testing). Understanding the potential releases from casks that could result from a human initiated event rests on knowing how these casks react to attack conditions.
- **Use a meaningful NEPA process regarding rail access.** Nevada has recommended that DOE use a credible National Environmental Policy Act (NEPA) process to select a preferred Yucca Mountain rail access corridor and rail alignment in Nevada. As the end point of a national transportation program, such a corridor is critical in the overall performance of the Yucca planning. The safety and security challenges that arise from building an extensive rail spur into the Yucca facility demand a robust dialogue on the issues, one that NEPA requires and to date DOE seems unwilling to offer any realistic approaches to studying. For example, the NEPA process DOE employed to select the Caliente rail corridor failed to adequately and consistently evaluate potential rail corridors.
- **WEIB "Straw man" Shipment Routes.** Nevada has recommended that DOE select routes for the national transportation system using a reasonable transportation methodology developed by stakeholders. Transportation safety and security require that DOE first plan what routes will be used so that meaningful stakeholder input can be focused on the planning. The DOE should follow a three-step process proposed by the Western Interstate Energy Board (WIEB):
    - DOE would designate "straw man" routes, preferably in a national level transportation NEPA document.
    - Member states would individually and collectively evaluate the DOE routes, and then designate preferred routes on a regional basis.
    - DOE would then formally adopt the routes selected by WIEB, and designate these routes (allowing exceptions for use of designated alternative routes in emergency situations) in DOE contracts with rail and highway carriers.

- **Start the Section 180(c) process.** Nevada has recommended that DOE implement the transportation planning and emergency response training program, required under Section 180 (c) of the NWPAA, through formal rulemaking. Absent rulemaking, the State of Nevada believes that congressional action might be needed to implement the program, as was the case with the Waste Isolation Pilot Plant (WIPP) DOE-State cooperative transportation planning program. The connection to safety and security is especially important here, without systems of well funded emergency response training the transportation program is seriously flawed. One of many safety and security issues: States would be facing an unfunded mandate to provide ~50 years of training, protection and response capabilities for the Yucca program. In terms of response capabilities and organizational capacity this would entail three or perhaps four generations of human capital with experience and knowledge of the program's operational parameters.
- **Respect State, Local, & Tribal Regulation.** Nevada has recommended that DOE support state regulatory enhancements to manage transportation risks and address public perceptions of transportation risks. These would include, but not be limited to:
    - Port-of-entry inspections and state escorts for DOE shipments at DOE expense.
    - States, in conjunction with local governments, may also impose seasonal, day-of-week, and time-of-day restrictions on DOE to address unique local conditions.
    - Tribal governments may also regulate DOE shipments.
- **Address issues associated with Terrorism and Sabotage.** Nevada has recommended that DOE address acts of sabotage and terrorism against repository shipments. DOE has acknowledged, in the Final EIS for Yucca Mountain, the potential vulnerability of shipments to such attacks. Analyses by Nevada contractors have concluded that the releases and consequences could be many times greater than reported by the DOE, resulting in catastrophic cleanup and recovery costs. NRC has likewise neglected its mandate as a regulatory body with respect to this issue. Specifically:
    - DOE needs to systematically address terrorism issues and risks in development of repository transportation operational protocols.
    - NRC has yet to respond to the specific terrorism risks and impacts documented in Nevada's 1999 petition for rulemaking (Docket PRM 73-10).

Since today's hearing is directly related to the last issue of concern, the balance of the body of this presentation will offer a methodology that could be used by the DOE, if it proceeds with the Yucca project, to assess and mitigate the risks of human initiated events like terrorism, sabotage, large scale protests and similar risk inducing events.

HUMAN INITIATED EVENTS AND SYSTEMATIC RISK ASSESSMENT

This portion of the testimony recommends the development of a comprehensive human initiated event threat assessment process for the proposed Yucca Mountain transportation system.[10] This process could be used by DOE to assess repository transportation impacts as part of its NEPA requirements, and in responding to the Western Governors Association (WGA) resolution on terrorism and sabotage.

This section identifies ways to improve current risk assessment techniques to meet the challenges of human initiated events, including terrorism, sabotage, induced or deliberate accidents, and violent protests. The recommended threat assessment process is presented as a series of industry standard methods and concludes with exemplar scenarios. The testimony is based only on open source data to develop these ideas, concepts and methodologies.[11]

Shipment Vulnerability Debate

For three decades, risk analysts have debated the vulnerability of spent nuclear fuel shipments to acts of terrorism and sabotage. The details of the debates are documented in studies prepared for the State of Nevada in 1998 and 2005.[12] The sabotage related attack scenarios evaluated in NRC and DOE analyses have changed little over the decades. The DOE/NRC analyses assume that a single spent fuel shipping cask is attacked at one location, by one group of attackers, using one weapon. The basic analyses assume that the attack breaches the cask and releases a small fraction of the contents. In general the agency sponsored analyses differ in estimates of the amount of radioactive material released, the details of the release and dispersal, the area contaminated, the population exposed, the resulting human casualties, and the economic impacts.

The first NRC regulations requiring physical protection of spent fuel shipments were issued in response to a 1977 draft assessment by Sandia National Laboratories (SNL). That assessment, and a follow-up study by SNL in 1980, indicated that sabotage of a shipment in an urban area could cause hundreds to thousands of casualties, and billions of dollars in economic losses and cleanup costs.[13] The NRC issued interim physical protection requirements for spent fuel shipments in 1979, and adopted the current system of regulations (10CFR73.37) by rulemaking in 1980.

Subsequent studies sponsored by NRC and DOE sharply reduced the estimated causalities and economic losses from this original scientific work product. The debate over the consequences of a successful terrorist attack resumed in 1984, when the NRC, acting on the new studies, issued a proposed rule eliminating physical protection requirements for most spent fuel

shipments. The NRC had concluded that the expected consequences of a successful attack in “a heavily populated area such as New York City would be no early fatalities and less than one (0.4) latent cancer fatality.” This NRC proposed rule was opposed by state governments, environmental groups, and some nuclear industry sources. Three years later, the NRC terminated the proposed rule, without explanation. Throughout the 1990s, however, the NRC continued to downplay attack consequences. At the same time, public discussion of vulnerability and consequences temporarily subsided.

The controversy re-emerged nationally in 1995 as the DOE began the NEPA scoping process for the proposed Yucca Mountain geologic repository. State governments and other parties urged DOE to more directly address terrorism and sabotage in the Yucca Mountain environmental impact statement (EIS). In its role as a stakeholder, the state of Nevada filed detailed scoping comments on the impacts of terrorism against repository shipments during 1995, and published several supporting studies between 1996 and 1998. Based on these studies, Nevada's Attorney General filed a petition for rulemaking with the NRC in June 1999. The Nevada petition documented the vulnerability of shipping casks, and argued that shipments to a national repository would create greater opportunities for terrorist attacks and sabotage**.** The petition, which requested strengthening of the current regulations and a comprehensive reexamination of radiological sabotage, was endorsed by the Western Governor's Association (WGA). More than eight years later, the NRC has still not officially responded to the Nevada petition.

DOE acknowledged that shipping casks are vulnerable to terrorist attack in the 1999 Draft EIS for Yucca Mountain.[14] In support of the Draft EIS, DOE sponsored a 1999 SNL study of cask sabotage, which demonstrated that high-energy devices (HEDs) were "capable of penetrating a cask's shield wall, leading to the dispersal of contaminants to the environment." The SNL study also concluded that a successful attack on a truck cask could release more radioactive materials than an attack on a rail cask, even though rail casks would contain, on average, up to six times more SNF than truck casks.[15]

In the 2002 Final EIS for Yucca Mountain, DOE updated its sabotage analysis, assuming more highly radioactive SNF, a larger respirable release, and a higher future average population density for U.S. cities.[16] In this document the DOE estimated that a successful attack on a truck cask in an urbanized area under average weather conditions would result in a population dose of 96,000 person-rem and 48 latent cancer fatalities. For a successful attack on a large rail cask, DOE estimated a population dose of 17,000 person-rem and 9 latent cancer fatalities. In neither case did DOE evaluate any environmental impacts other than health effects, and ignored the economic impacts of a successful act of sabotage. While the DOE did not specifically estimate cleanup costs after such an attack, the FEIS states that clean-up costs following a worst-case transportation accident could reach $10 billion.

Analyses prepared for the state of Nevada by Radioactive Waste Management Associates (RWMA) calculated that sabotage impacts could be considerably greater.[17] RWMA replicated the DOE Final EIS sabotage consequence analyses, using the RISKIND model for health effects and the RADTRAN model for economic impacts, the SNL study average and maximum inventory release fractions, a range of credible values for the gap inventory of Cs-137, and a range of population densities and weather conditions.

RWMA concluded that an attack on a truck cask using the same common military demolition device assumed in the DOE analysis could cause 300 to 1,820 latent cancer fatalities, assuming 90% penetration of the cask by a single blast. For the same device used against a large rail cask, RWMA estimated 46 to 253 latent cancer fatalities, again assuming 90% penetration. The major radiological health impacts of an attack would be caused by the downwind dispersion of respirable material (mainly particles with a diameter less than 10 microns) that could be ejected from the damaged cask. Depending upon the meteorological conditions present at the time of an attack, the respirable aerosol of radioactive materials could affect an area of 10 square kilometers (3.9 square miles) or more. RWMA estimated cleanup costs ranging upward from $668 million for the rail incident, and $6.1 billion for the truck incident, to more than $10 billion. Full perforation of the truck cask, likely to occur in an attack involving a state-of-the art anti-tank weapon, could cause as many as 3,000 to 18,000 latent cancer fatalities, and cleanup and recovery costs could far exceed $10 billion.

In October 2007, DOE published the Draft Supplemental Environmental Impact Statement for Yucca Mountain (DSEIS) and the Draft Rail Alignment Environmental Impact Statement (RA DEIS).[18] Both the DSEIS and the RA DEIS address the impacts of sabotage against repository shipments. In both volumes DOE states that it has "analyzed plausible threat scenarios, required enhanced security measures to protect against these threats, and developed emergency planning requirements that would mitigate potential consequences for certain scenarios. *DOE would continue to modify its approach to ensuring safe and secure shipments of spent nuclear fuel and high-level radioactive waste, as appropriate, between now and the time of shipments.* For the reasons stated above, DOE believes that under general credible threat conditions the probability of a sabotage event that would result in a major radiological release would be low" (DSEIS, p. 6-22; RA DEIS, p. 4-314, *emphasis added*).

Acknowledging "the uncertainty inherent in the assessment of the likelihood of a sabotage event," the DSEIS and RA DEIS evaluated events in which "a modern weapon (high energy density device)" is used to "penetrate a spent nuclear fuel cask." DOE evaluated the consequences of events occurring in representative urban, suburban, and rural areas. Based on new research by Luna (2006)[19] and on European studies, the DSEIS assumed that the single weapon attack studied would result in a smaller release of respirable material than DOE

assumed in the 2002 FEIS. For a sabotage event against a truck cask in an urban area, the DSEIS reports consequences about half what DOE estimated in the 2002 FEIS - a population dose of 47,000 person-rem, and 28 latent cancer fatalities. For an attack on a large rail cask in an urban area, the DSEIS reports consequences about double what DOE estimated in the 2002 FEIS - a population dose of 32,000 person-rem, and 19 latent cancer fatalities.

The DSEIS does acknowledge the aforementioned State of Nevada analyses under the heading "Transportation Sabotage: An Opposing Viewpoint." Despite this note in the document, and as in earlier DOE analyses, the DSEIS does not provide specific information on:

- The land area contaminated.
- Economic losses due to disruption of normal activities.
- The cost of cleanup.

As of 2008, the State of Nevada is preparing its own detailed reassessment of transportation sabotage impacts. To date, Nevada has submitted comments on the DSEIS sabotage consequence analyses (January 10, 2008). In those comments, Nevada emphasized that the DSEIS continues to ignore the consequences of a terrorist attack using one or more weapons that completely perforate the shipping cask, or a combination of weapons specifically designed to breach, damage, and disperse the cask contents. Such an attack could result in impacts more severe than those evaluated by DOE.

The new DOE sponsored research does not address such impacts. In fact, the Venturi effect created by full perforation of a shipping cask would likely negate the reduction in impacts claimed in the Luna (2006) study. In its key conclusion, DOE asserts that the factors identified by the State of Nevada "could affect the chances of success but not the outcome of the sabotage event."[20] DOE presents no evidence in the DSEIS, the RA DEIS, or any of the cited references to support that assertion.

Moreover, the DSEIS ignores evidence, including terrorism studies funded by DOE that this agency's activities may be particularly attractive symbolic targets for sabotage or terrorist attacks. The DSEIS also ignores past instances in which human errors in cask fabrication and cask loading actually occurred during NRC-licensed shipments, and created conditions that could have compromised cask performance in the event of a sabotage event. Likewise, the DSEIS ignores Nevada's argument that unique local conditions such as proximity of the existing mainline railroads to urban location like downtown Las Vegas and Reno-Sparks must be factored into consequence assessments, resulting in potential multi-billion dollar cleanup costs and business disruption impacts.

In summary, all of the consequence assessments so far conducted by NRC, DOE and the State of Nevada assumed single-phase attack scenarios. None of these consequence assessments have evaluated the effects of an attack involving the simple impact-exacerbating tactics identified by the U.S. Army peer review report more than two decades ago: namely the combined use of a breaching device and a dispersal device, or use of multiple breaching devices. None of these consequence assessments have incorporated insights obtained from the 1998 testing sponsored by International Fuel Containers, Incorporated, at the U.S. Army Aberdeen Test Center in which a newer generation weapon, a TOW II warhead, was used. Most significantly, none of these consequence assessments have evaluated any of the impact-exacerbating tactics studied by counter-terrorism experts in the post-9/11 threat environment. Credible hijack and control scenarios, specialized truck bomb scenarios, and/or concealed weapons like IED's (improvised roadside devices), coupled with insider assistance, diversionary attacks, and/or suicide tactics, could potentially result in radiological consequences far greater than those previously estimated by NRC, DOE or the State of Nevada.[21]

WGA Resolution

The primary motivation for this suggest analytical format, prior to publication of the DOE's DSEIS, was the WGA resolution regarding Yucca Mountain transportation. The WGA represents nineteen Western states and three territories. The association allows state political leaders to address critical policy issues in a wide variety of areas. The WGA organization thus helps state leaders develop strategies to address complex issues facing western states.[22] WGA has been actively involved in nuclear waste transportation planning for two decades. In 2007, WGA renewed and revised a policy resolution (07-2) on the risks of terrorism and sabotage against repository shipments.[23] The original resolution behind this new document had been adopted in 1998.

WGA Resolution 07-2 notes that in the aftermath of the September 11, 2001 terrorist attacks, *the altered threat environment calls for new, more comprehensive terrorism assessment tools.* The resolution calls upon the NRC to "fully address the consequences of attacks against all components of the nuclear waste handling and transport system, to include: attacks against transportation infrastructure, the theft of a shipment, use of high-energy explosives against a shipment cask, and direct attacks against a shipment cask using antitank missiles or other armament that could cause a loss of containment." WGA further requests that NRC "strengthen its efforts to share information with state and local governments regarding spent fuel shipment vulnerabilities and consequences, " recognizing that "sharing of information must be conducted within the framework of preventing the release of sensitive or classified information to individuals without a need to know."

The WGA resolution notes that DOE has acknowledged the vulnerability of shipments in the 2002 Final EIS for Yucca Mountain. The resolution states: "DOE should continue to address acts of sabotage and terrorism in its NEPA documents, and should incorporate terrorism/sabotage risk management and countermeasures in all DOE transportation plans, protocols, and practices relating to operation of a repository, interim storage facility, and/or intermodal transfer facility, including liability for costs and damages resulting from terrorism/sabotage against nuclear waste shipments. DOE should share security-related information with state and local governments to the maximum extent practicable."[24]

Comprehensive Threat Assessment

Driven by regulations and the need to protect the public from catastrophic events, the nuclear industry has a continuous quality improvement process for security against human-initiated events. The two recently issued DOE NEPA documents, the Draft Supplemental EIS and the Draft Rail Alignment EIS, employ only some of the methods used by the industry to protect fixed assets like reactors, but the not expressly documented analytical method employed by DOE for the Yucca Mountain transportation effort *does not use state of the art assessment techniques, nor does the assessment effort meet industry standards for fixed site security.*

The problem with the DOE's approach to the NEPA documents (SEIS's) is two-fold: How to assess the threat of human-initiated events against spent fuel shipments to Yucca Mountain nationally, and secondly, for the proposed Caliente rail line in Nevada. Once again, human initiated events refer to the range of malevolent acts that could be perpetrated on the shipments – including such events as terrorism, sabotage, deliberate accidents and violent protest movements.[25] Shipments refer to the various means that will be used to move SNF and HLRW into the national transportation system/proposed Caliente rail corridor from their current storage facilities at commercial nuclear power plants, DOE weapons production sites, and from other DOE serviced/regulated/owned source facilities.

This presentation recommends specific and detailed methodologies that are used in social science and industry that, that taken together, could constitute a comprehensive threat assessment for the proposed Yucca Mountain transportation system:

- The identification of relevant human-initiated events by use of meta analysis.
- Development of a systematic multi-level assessment of human-initiated event risks for the transportation modes, facilities, corridors, etc.
- A resultant matrix of human initiated events and attack scenario exemplars suitable for DOE study and consideration in NEPA documentation.

Human-initiated events

Several large categories of human-initiated events can be identified across the major components of the transportation system and relative to the known or expected characteristics of the Yucca Mountain transportation system. These include terrorism, sabotage, accidents and protests.[26] The table below lists these four event categories and notes how they may apply to the four major transportation components derived from the DOE "Transportation Concept of Operations" and DOE "Draft National Transportation Plan".[27]

Figure 2: Human Initiated Event and transportation Activity Matrix

Threat Categories	Origination Point	Transport Activities	Transfer Facilities	Destination Facilities
Terrorism Attacks	X	X	X	X
Sabotage	X	X	X	X
Deliberate Accidents	X	X	X	X
Violent Protests	_	X	X	-

Terrorism attacks are defined here as those malevolent actions that are designed to cause significant symbolic events, a significant incident that acts as a statement in opposition to the shipments or an act that directly attacks the transports, casks, facilities for handling shipment casks or the personnel that are involved in the four categories of transportation infrastructure noted above. These terrorism acts will range on a continuum from symbolic events that are not intended to result in a release of radioactive materials all the way up to sophisticated full-scale assaults designed to release/disperse the casks radioactive contents. These attacks may be motivated by a political/social/religious agenda, attacks prompted by an anti-federal government agenda, attacks based on the deliberate creation of economic dislocations in the energy sector, or attacks that are inspired by a social issue. These attacks may be perpetrated by foreign nationals, American citizens, or any combination of the two.

Sabotage is defined herein as those malevolent activities that could interfere with the safe and secure loading/unloading and transportation of the nuclear wastes. Examples may include the use of insider

information, employee tampering with casks, large scale labor problems, and/or deliberate contamination of casks/transports to delay shipments. Sabotage can also be defined as activities detrimental to the safe and secure transport of these materials. Sabotage acts will also exist on a continuum from attacks not intended to damage a cask up to an act designed to release/disperse the inventory of radionuclides. The motives for such attacks are considered to be the same as for the terrorist attacks and acts of sabotage may be perpetrated by the same range of adversaries.

Deliberate Accidents are defined here as those malevolent human-initiated events that result in endangerment of the shipments, their casks, or the overall shipment campaign. These may come from deliberate acts by an individual or small group interfering with shipment operations and from negligent acts of those within the transportation system that can create a potential, minimal or significant release of the highly radioactive contents. Like terrorism and sabotage, these acts will also exist on a continuum from attacks not intended to damage a cask up to an act designed to release the inventory of radionuclides. The motives are considered to be the same as for the terrorist attacks and they may be perpetrated by the range of adversaries.

Violent Protests are defined as those potentially malevolent activities that could interfere with the safe and secure transportation of the nuclear wastes. These protests may also be used as a rouse to hide the intentions of malicious actors who seek to commit acts of terrorism or sabotage by hiding their actions in the larger protest group. This category is included to recognize the fact that these shipments will face significant opposition from protesters, based on the experiences of other shipment campaigns around the world. Such large scale protests may endanger the shipments and/or public health by delaying shipments and increasing routine doses to the population. These acts will also exist on a continuum from collective acts not intended to damage a cask up to an act designed to release the inventory of radionuclides. The motives for such attacks are considered to be the same as for the terrorist attacks and they may be perpetrated by the same range of adversaries.

Threat Assessment Process

A range of threat assessment procedures should be conducted prior to commencement of shipments and continued during the shipping campaign, in a way that measures risk over time, and enables assessments to be continually updated.[28] The longitudinal risks may also need to be assessed because of a rise in energy related terrorism acts,[29] and as part of the on-going DOE obligation to operate under procedures equivalent to the NRC physical protection regulations (10CFR73.37), although DOE is not necessarily subject to these particular NRC regulations.

Meta threat analysis

The analysis-in-depth suggested herein starts with consideration of a wide range of potential threats and consequences via-a-vie shipments. Such a systematic assessment would first involve an exhaustive meta-analysis of the literature relative to attacks on shipments of hazardous materials, including SNF and HLRW. This process would need to account for emerging threats and tactics being employed by terrorists/adversaries around the globe. It would also include IAEA (2007) guidance documents on the subject and documentation of threats that have arisen in the global theater where terrorists/adversaries

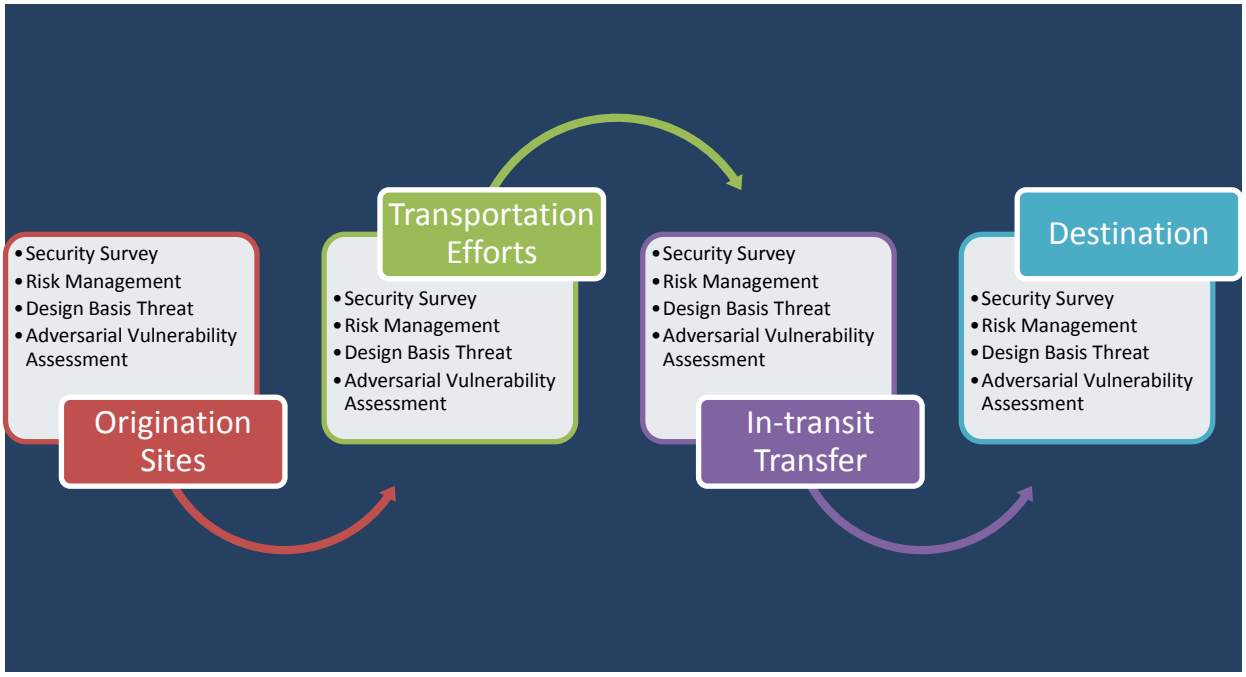
operate. This data should then be vetted with outside stakeholders, not just internal DOE security personnel, to define the various challenges that the Yucca Mountain transportation effort could face over the five decade life span of the proposed project. Emerging from this effort would be a pro-active catalogue of transportation risks and issues that should inform a NEPA analysis, not just cherry-picked scenarios that react to the latest criticisms, from Nevada studies, government analysis and/or those generated by the National Academy of Sciences.[30]

Vulnerability Assessment Process

Transportation security for a cargo as dangerous as the highly radioactive SNF and HLW should prompt planners to use the best available techniques to reduce threats from human-initiated events. Typically security professionals use four levels of vulnerability assessment techniques to protect nuclear facilities and other critical industrial applications.[31] Each of several techniques has strengths and weaknesses but with the combined (triangulated) use of all of these techniques, taken together as a NEPA inspired research strategy, allows for improvements in security and better defines risks. That is, the use of more than one of these offers a more robust methodological approach to the task at hand, all of them allows for a form of defense-in-depth, a common principle in nuclear security.

These four techniques offer a comprehensive risk identification and mitigation potential for security (and safety) issues relative to the proposed Yucca Mountain transportation program. In order to use these techniques it is first useful to identify where they may apply to the overall transportation effort. The following chart helps situate these four techniques relative to the four major components of the transportation infrastructure.

Figure 3: Transportation analysis-in-depth: Risk reduction strategy



The examination of how these four identification, reduction and mitigation techniques can be used in the systematic assessment of risk for the Yucca Mountain project, the analysis-in-depth risk reduction concept noted above, will require some details on what each technique will entail in real world practice.

First, it is critical that they should be considered an integrated system of analysis, albeit one with some level of analytical hierarchy. The following chart demonstrates their interrelationship and the preferred hierarchy.

Figure 4: Analysis-In-Depth Concept; Sub-Components

Security Surveys. Security surveys are the first level in this overall transportation risk assessment schema. These surveys represent a physical examination of the transportation security arrangements and typically use a check list approach to the examination of risks. This allows for the standardization and management of the assessment process.[32] These checklists aid security efforts and provides for a consistent, albeit unimaginative examination of risks.[33] This form of security management is typical for any number of industrial applications and has a long tradition in security. At a minimum this survey technique needs to be performed at various levels of the proposed Yucca Mountain transportation effort (for example at origination sites, for transportation efforts, at in-transit transfer facilities, and for destination conveyance infrastructures).

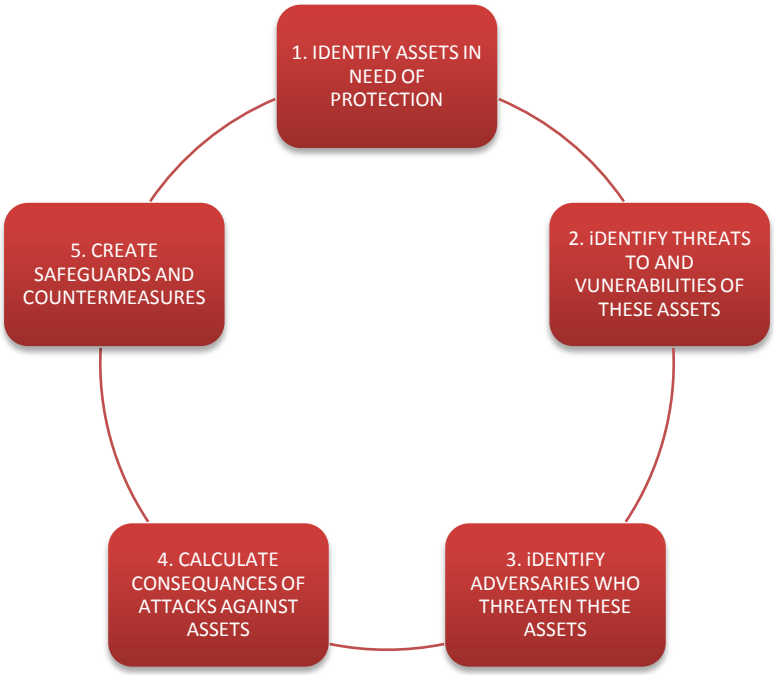
The problem with this technique is that it is typically not focused on the adversaries and does not necessarily encourage thought relative to new countermeasures as risks change over time. In fact

surveys become reified and represent a binary (good/bad, black/white) approach to security and risk mitigation. They seem to imply that risks will somehow emerge from the world and show themselves during such surveys. Checklists are also fixed lists of observations to be conducted and typically closed to emerging risks that have heretofore not been known or overlooked. The list becomes what human assets are fixated on, not focusing security personnel on the creative protection of the cargoes, rather making them focus on paperwork. These surveys are often misused, especially when they come to represent ways to manage people and ensure compliance to a security regime or regulations.[34]

Security surveys have a place in the overall transportation efforts but they are not in and of themselves a cure for the risks that transportation efforts to Yucca Mountain will face. They represent a tool that should be employed by those involved in the transportation effort and at all levels of the transportation infrastructure. They are the first line of defense since they are carried out traditionally by line staff and management. They also require periodic updates, monitoring and analysis as to their ability to meet current challenges and contemporary threats. They represent the first line of a transportation specific defense-in-depth concept yet to be adopted by DOE.

Risk Management. The second step in the analysis-in-depth risk assessment process is to use well understood and common place risk management techniques. The process of risk management is fairly straightforward. In the first phase of the risk management process the analyst begins with identification of the assets in need of protection and ends with the identification of safeguards and countermeasures.[35] Thus, the organization using the risk management technique should basically follow the flow of the following interrelated items:

Figure 5: Risk Management Process



After this largely abstract intellectual task is completed, the organization then uses an expert opinion process to rank order priorities and probabilities are assigned to each sub-phase noted above. Typically this involves predominantly quantitative outcomes and these outcomes are summarized in tables, charts, and the like. Thereafter the transportation management team would appropriate, and field, security resources accordingly. As implied by the chart, the process begins anew once this final task is completed and in practice should become a never ending series of assessments designed to improve the overall robustness of security.

Risk management is not without critics in the nuclear field and elsewhere. Some argue that the traditional ways of conducting risk management need to be more quantitative or address more aspects than are traditionally used in such analysis,[36] while others note the political nature of the use of risk management.[37] A systematic examination of risk management also reveals some issues of concern.[38] Once again this technique is typically binary and closed to outside input. For example, there is rarely outside input on contemporary threats and vulnerabilities since risk management rests on known (historic) security issues. This means that risk management is reactive, not proactive in mitigating risks. This also usually means that risk management is done without the creative spirit that the terrorists/adversaries bring to the table. If it is initiated, managed and used by organization staff in agencies (for example the NRC and DOE) and represents the collective consensus of these sometimes limited perspectives.

Risk assessment is rarely the creative expression of alternatives. Risk management is management of risks by managers and for managers. It is not done from alternative perspectives (for example the adversaries). The assignment of probabilities in risk management is often based on fantasy-like numbers that are created out of thin air to placate internal constituencies and/or to serve political purposes. Once these probabilities are codified in tables, charts and the like, they become real in their consequences as everyone involves start to believe they are real and act accordingly.[39] The process itself and especially the documents that emerge create overconfidence in the numbers, a false sense of security that is problematic in the face of real world creativity from adversaries.

Risk management has its place in transportation planning for the potential Yucca Mountain program and the problems noted here do not negate its usefulness. As a technique it is not a be all and end all in risk assessment. The use of quantitative data helps policy makers believe in a program, but that is a two edged sword.

Design Basis Threat (DBT). The third level of the analysis-in-depth paradigm is the DBT. In some respects the DBT is a technique not that unrelated to risk management.[40] A DBT is a proxy threat, a hypothetical scenario based on descriptions of the threats found at the time of its articulation.[41] The DBT sets the standards for security personnel by defining the training, weapons and tactics that a terrorist/adversary group could use to attack nuclear facilities. The best practices of DBT usage call on its proponents to design security to face the contemporary threats, recognizing vulnerabilities and to allocate resources accordingly.[42] DBTs tend to focus on infrastructure and physical security hardware, more so than risk management.[43]

The published DBT details for nuclear power plants serve as an illustration of this process and its outcomes. The DBT has been used since the 1970's in the United States and is not a single process. It has also been used in various ways by different countries as the IAEA seeks to standardize the process around the globe. First and foremost it is the basis of physical protection systems (PPS) for *fixed* sites. It also serves as the means by which an evaluation of that PPS is conducted. Since 2000 the IAEA has promoted the DBT and provides (in conjunction with Sandia National Labs) nine steps for the process of development, use and maintenance of a DBT system. Besides the basic facts noted in this paragraph certain scholars[44] suggest that a DBT generally includes:

- ✓ Identification of the roles and responsibilities within and connected to the organization.
- ✓ Development of operating assumptions for the usage of the DBT.
- ✓ Identify a range of potential generic adversary threats.
- ✓ Identify a list of threat characteristics.
- ✓ Identify sources of threat information.
- ✓ Analyze and organize threat-related information. (Steps one to six create a threat assessment document).
- ✓ Develop threat assessment and gain consensus about said.
- ✓ Create a national level DBT.
- ✓ Introduce the DBT into the regulatory framework.

The DBT process, and specifically its first six steps, should yield both motivations for attacks, intentions of the attackers and characteristics of the attacking force. These are then matrixed across a range of adversaries (protesters, activists, extremists, criminals and terrorists). In most cases these are created from assumptions based on historic data and firmly rooted in a philosophy that insists that all threats must be "credible." This philosophy is counter intuitive to 9/11 threat realities and may blind the creators to new/emerging threats or threats that are evolving as past threats change to meet new circumstances. Typically the DBT philosophy does promote the continuation of the status quo.

The NRC and DOE have updated their DBT in the aftermath of the 9/11 attacks, once in 2003 and again in 2004, both times in a process outside the normative framework for such adjustments. Specific details are not known for these classified documents but the expectation is that they will take years to implement a new DBT and that the final product was diluted as a result of industry concern over costs. Likewise, the DBT has been criticized since it does not meet the threat threshold the 9/11 attacks presented.[45]

DBTs have their critics and the criticisms run along similar lines to those for the risk management techniques.[46] The DBT is a typically binary process and closed to outside input, primarily for security reasons like classification of results. Because of the closing of discussion for security reasons, there is

rarely outside input on contemporary threats and vulnerabilities. Secondly, like risk management the DBT becomes a reactive device. As a proxy attack strategy it is not proactive in mitigating risks. Similar to risk management the DBT process is dominated by the organization staff. The DBT represents the collective consensus of these limited and sometimes self-serving perspectives. It does not represent a creative expression of alternatives and rarely addresses emerging threats. Once the DBT is determined it becomes real in its consequences for the agencies using this technique. The threat is what the DBT says it is, nothing more or nothing less. The DBT provides insider organizations, although not the public and other stakeholders, with a sense of confidence that may be disproportional to the risks and reality of a changing world. It allows an existing organization like the DOE to define what the threats are, and once the DBT is constructed, to maintain a faith in their assessments, a self fulfilling belief system that can be dangerous when one is protecting something as potentially dangerous as highly radioactive wastes.

In some cases critics have argued for a layered approach to DBT implementation, a strategy that recognizes financial resource differentials in government's responsible for implementation.[47] This criticism is primarily focused on less developed nations where the resources necessary to protect nuclear assets are not readily available. In the case of advanced industrial nations the AHARA – as high as reasonably achievable - principle behind such debate suggests that these nations should achieve the IAEA's goals of securing radioactive materials against human-initiated events. These less than reasonable security debates do not apply to the United States, a country rich in resources.

Additionally, as noted DBTs are supportive of the status quo. They seem to say to everyone involved we are doing good, look how hard we worked to define the threats and our perceptions of the vulnerabilities we face are excellent. It ignores alternative threats since they are deemed too improbable or they are not perceived at all – they are deemed a very subjective 'uncreditable.' The DBT seems to communicate to one and all that whatever terrorists/adversaries can do poses a lesser threat than our proxy measure (DBT), a dangerous oversimplification in the post 9/11 world of nuclear security.

DBTs also take time to change, they are not assessed systematically but rather on an as needed basis. The DOE mandated and NRC inspired changes in implementation for weapons production facilities and commercial nuclear power plants after the 9/11 terrorist attacks illustrate this delay – changes in the DBT were revised in 2003, changed again in 2004 and are still undergoing implementation as of the seventh anniversary of those attacks with an expected date for completion being in 2008.[48] Supporters argue that a change in the DBT is costly but critics point out so too would be a successful attack.

The DBT is a step forward from past risk assessment practice and one that allows transportation managers to create a proxy for security to train against. It is different than security surveys and risk management, but it is not the single magic bullet to security. Rather the DBT is one tool in the overall toolbox for risk mitigation. The fourth technique, adversarial vulnerability assessment, helps with some of the limitations noted for DBTs.

Adversarial Vulnerability Assessments (AVA). One critical omission of all three of the techniques detailed above is bringing the motives, mindset and creativity of the adversary into the risk equation.

Those who would wish to perpetrate a human-initiated event are far more resourceful than the security surveys, risk management and DBT techniques seemingly give them credit for. To accomplish the task of recognizing such creativity Johnson (2005)[49] advises that it is necessary to conduct a "mental coordinate transformation." This means that when assessing risks for critical SNF and HLW transportation infrastructure it is necessary to think like the perpetrators, not like security professionals, not like energy company officials, and not like oversight agency management.

The major barrier faced by security professionals and risk managers in doing this task is that they are rarely prepared for this mental transformation. As a result of organizational socialization they cannot, or will not, use the opportunity to actively look for threats, to engage in the alternative and/or to think like the terrorist, saboteur or other perpetrator of human initiated events. They have difficulty letting the opponent define reality, a reality that is securely planted in their professional lives by the very industry they seek to protect – one that for many reasons does not admit gleefully to risks, threats or terrorism as a potentiality. Altering Johnson's (2005)[50] approach for the proposed Yucca Mountain transportation project would entail the necessary mental transformation for the NEPA assessment. This is best accomplished by the following steps:

- Understand the full scope of the transportation effort. This includes all aspects, parts, components and variables in the transportation system. This is difficult since the totality of the system is enormous and in many cases individuals are asked to transform their thinking while working on small parts of the overall picture. Still it is necessary since the parts are integrated and the risk synergy for the total system far outweighs the singular transportation component risk level.

- Brainstorm in a creative, innovative, and multi-level manner that allows you to not just identify a threat, but to focus attention to a range of threats. [51] Once the totality of the program is recognized, members of a risk focus group are gathered to work on the issues, share their insight into the risks, and to brainstorm on threats facing this transportation system. These discussions would reveal attack exemplar scenarios tied to risks, not singular as is the case of a DBT, but multiple threats and with multiple consequence profiles.

- Once attack sceneries are identified, the group starts to edit these down to essential elements and exemplars that demonstrate vulnerabilities of the system, not just a single part of this complex transportation effort. This group would prioritize potential attacks which represent a range of possibilities, consequences and potential responses. These alternatives must be developed, articulated and vetted with a wide range of constitutes/stakeholders to gain additional insight and to reduce the problems of group think and collective risk blindness that sometimes arise in small groups.

- The last step is to determine the feasibility of these attacks by means of a range of attack articulations, analyze radiological consequences of these alternatives and devise countermeasures to mitigate these risks.

Several provisos are offered to those considering adopting AVA methods. First and foremost, let those involved be creative.[52] In the case of terrorism threats, the changes in technology, availability of information and tactical knowledge of adversaries demand that those involved be allowed freedom to achieve this creative approach to risk assessment. Historical data, and historically situated risk perceptions, are less significant in the face of global social challenges like currently are transpiring, a point often missed by those who work in formal organizations. AVA risk measurement is predicated on creativity which must be combined with organizational experience, technological skills and bureaucratic imagination. All of these tasks are difficult for many formal organizations to engage in but the challenges they pose are important to overcome.

Johnson (2005)[53] advises that creativity is the domain of individuals, not formal organizations. Good group dynamics can enhance this individual creative spirit and groups need to be involved to prioritize and determine feasibility. One of many techniques to help this creative process is to reverse engineer the attacks in an effort to solve problems that have yet to arise. This is a particularly cogent piece of advice given the elongated timeline for the proposed Yucca Mountain project and points out the need for a systematic longitudinal analysis paradigm so that data can be gather to inform the processes.

One of the most interesting advisements offered is that the system conducting this analysis must bring in outsiders and not use the typical cast of insider characters who have vested interests in the status quo. The use of the same old energy industry insiders and the same supporting industrial infrastructure insiders ensures the same old results. It does not offer a creative analysis of threats. Furthermore it is necessary to combine these outsiders with *creative* insiders in the brainstorming groups and set ground rules for all the contributors. These ground rules have to allow for all manner of input and treats each contribution as significant, be it from inside or outside the typical organizational patterns of thought. Johnson (2005)[54] offers some AVA imperatives as guidance. These have been modified to the Yucca Mountain project and include:

- Minimize the conflicts of interest and reduce wishful thinking on the parts of group members.
- To promote creativity in the group processes, the system must not punish those who creatively deconstruct its assumptions, bias, and working relationships.
- The overall group and its work product need to be assessed by a second group of outsiders, called assessors. These assessors should be independent from the Yucca Mountain project, experienced in finding problems and offering solutions, and in no small measure represent the public stakeholders for the project.
- All parties involved must discard the binary way of viewing risks. This means individuals need to be able to work within the gray areas of life, not the rigid confines of an engineering perspective or other professional paradigm that promotes the status quo philosophy.
- The group members are tasked with finding vulnerabilities and risks, which is their primary purpose. As such they should not be encouraged to find no vulnerabilities or no risks, a philosophy that is counter-productive to the AVA process.

- AVAs are not a pass or fail technique for the group as a whole and the group participants must be encouraged to reject this form of thinking. The point is to find vulnerabilities and risks, not fix them per say. Thus, finding these vulnerabilities and risks is a good outcome, not a negative outcome of the group process.

- The process must be done before transportation planning is fixed in policy, done again when plans are finalized but before transport begins, and done periodically thereafter (for example bi-annually or annually).

- AVAs are a holistic approach to vulnerability identification and risk mitigation. They should not be done in isolation (for example for the rail system alone).

- The conveners, participants and/or the assessors should not be restricted as to time, budget or attack possibilities. They should be allowed to creatively face the social context of global conditions relative to terrorism, sabotage and other human initiated events.

- The group should be encouraged to never underestimate the resourcefulness, creativity or commitment of the adversary. They should remember it is the adversary that defines the threat, not the protectors.

- The group should establish a hierarchy of threats, simplest to most complex, least severe radiological consequences to most severe radiological consequences. They need also look at contingencies that would take a second tier threat and make it a major radiological event. This is one area where DBTs seem to fail, they are based on one threat and do not necessarily account for such upgrades and modifications.

- Everyone should assume that adversaries know what security arrangements are in place, have the creativity to overcome these and/or will exploit those instances where the system does not meet its presumed minimum operation levels. Systems fail and human security systems fail to protect even the most critical of assets over time.

- A range of attacks should be considered by this group: terrorism, sabotage, probes of the security system, insider/outsider/insided-outsided threats, social engineering, and the many other varieties of human initiated events that could transpire.

- The longer a system is in place, the higher its vulnerability and risk to attack. Vigilance decreases with familiarity, hence the systematic reevaluation of risks becomes increasingly important over the lifespan of the program. It is equally important to note that once an AVA is complete, perhaps even deemed excellent by all involved, it is not the end product and cannot stand alone in the face of the ever-changing security threats faced. Once the AVA is complete it is then systematically and periodically subject to challenges from the original group, from new group participants and from new human initiated events/tactics.

- The group should avoid common nuclear industry fallacies. For example, many believe that all vulnerability will be discovered and thus all risk mitigated. Likewise they should be cautioned to avoid mindsets that see compliance as good security, layers of mediocre security equals good security, and/or that high-tech security is the answer for all vulnerabilities and risks.

AVAs are not the final and best answer to the reduction of risk, just as security surveys, risk management and DBTs do not tell the whole risk story. They are also not unknown to the nuclear industry. For example, they have already been used in the nuclear waste field for low level waste and relative to interim storage.[55] They also were advocated as one means to increase security after the terrorist attacks of September 11, 2001, and for use in critical infrastructure sectors like the chemical industry. [56] These techniques have even been around a sufficient length of time to note development in their applications.[57] Regarding their use in environmental policy debates, as has been the case with Yucca Mountain, Busenberg (1999)[58] notes they are effective in reducing policy disputes, a quality lacking in many suggestions for the proposed Yucca Mountain project. Lastly, these have been used in the energy industry for security considerations relative to oil and gas pipelines, a similar security dilemma to that posed by transporting nuclear waste across country to Nevada.[59]

The AVA is one tool in the overall risk assessment tool set necessary to secure the transportation of highly radioactive materials like SNF and HLW. Used in conjunction with the other three techniques it allows a different perspective on the problems the system may face, a valuable perspective not offered at any other time in the lifecycle of the transportation program.

Step Three – Scenario Exemplars

Analysis-in-depth is a management paradigm and an analytical imperative necessary to accomplish the formable task of vulnerability and risk assessment for the complex, decades-long transportation effort that would be necessary for the proposed Yucca Mountain repository. The following sections provide a risk matrix and corresponding threat scenarios that could emerge from an AVA process, if applied. The details and threats noted therein are gleamed from the literature and used to represent best practices in risk assessment for the proposed Yucca Mountain project. They do not directly correspond to the issues noted above; rather they examine a subset of the overall risk of human-initiated events for transporting nuclear wastes. The following matrix shows some of the potential human-initiated events identified for further study.

Figure 6: Potential Human Initiated Events for Further Study

Potential Events	Origination Sites	Transport Issues	In-transit Transfer	Destination Facilities
1. Labor disruptions with deliberate tampering of transports and/or casks. (SAB)	X	X	X	X
2. Deliberate contamination of transports and/or casks. (SAB)	X		X	
3. Disabling of shipment safeguards. (SAB)	X	X	X	
4. Actions meant to delay the shipment process and creating significant media attention. (PRO)		X	X	
5. Actions meant to delay transport and create increased routine radiological impacts. (PRO)		X	X	
6. Actions meant to create a dislocation of transport, cask or transportation infrastructure. (PRO)		X	X	
7. Use of geographically disadvantageous features along the transportation routes to impact shipments. (ACC)		X	X	
8. Exploitation of steep grades, tunnels, and bridges to create accident conditions potentially challenging cask integrity. (ACC)		X	X	
9. Inducement of inadvertent collisions involving toxic, explosive or flammable chemicals. (ACC)	X	X	X	X
10. Use of man-portable missiles to penetrate the cask and disperse the contents into the environment. (TER)	X	X	X	X
11. Use of military weapons/tactics to penetrate the cask and disperse the contents into the	X	X	X	X

environment. (TER)				
12. Use of adjacent transportation infrastructure and cargos to augment an attack and increase consequences.		**X**	**X**	
13. Capture of the cargo.		**X**	**X**	

Abbreviations: SAB = sabotage, PRO = protests, ACC= accident, TER = terrorism

The Risk Matrix

Considering the Yucca Mountain transportation options identified by DOE, five modes of transportation could potentially be used for repository shipments over the projected 50-year operations period. These include:

- Rail Casks Shipped by Rail.
- Rail Casks Shipped by Barge.
- Rail Casks Shipped by Heavy Haul Truck.
- Truck Casks Shipped by Rail.
- Truck Casks Shipped by Legal Limit Truck.

These five transportation modes, traveling to Yucca Mountain from 76 shipping sites in more than 30 states, with an average shipment distance greater than 2,000 miles, will be subject to many possible attack strategies over five decades. This approach uses a range of exemplar human-initiated event strategies as an illustration of the risks associated with the transportation of these materials. These include:

- Theft of the Cargo.
- Transportation Infrastructure Attacks.
- Anti-tank and/or Stand-off Weapons Attacks.
- Capture of Shipment and use of High-Energy Density (HED) Weapons.

These exemplars suggest that a range of consequences must be factored into risk assessment since they present a range of potential attack outcomes. These outcomes include:

- Attacks to Disrupt Shipments (Minimum Radioactive Dispersal).
- Attacks to Disperse the Cask Contents (Moderate Radioactive Release).
- Attacks for Maximum Consequences (Catastrophic Radioactive Release).

The following chart allows for the analysis of these various factors simultaneously and has estimates of the consequences listed in bold as they relate to the scenario analysis that follows.

Figure 7: Risk Matrix

Yucca Mtn. Risk Matrix	Rail Casks Shipped by Rail.	Rail Casks Shipped by Barge.	Rail Casks Shipped by Heavy Haul Truck.	Truck Casks Shipped by Rail.	Truck Casks Shipped by Legal Limit Truck.
Theft of the Cargo.	**Disrupt** Disperse Max. Cons.	**Disrupt** Disperse Max. Cons.	**Disrupt** Disperse Max. Cons.	**Disrupt** Disperse Max. Cons.	**Disrupt** Disperse Max. Cons.
Transportation Infrastructure Attacks.	Disrupt **Disperse** Max. Cons.	**Disrupt** Disperse Max. Cons.	Disrupt **Disperse** Max. Cons.	Disrupt **Disperse** Max. Cons.	Disrupt **Disperse** Max. Cons.
Anti-tank and/or Stand-off Weapons Attacks.	Disrupt **Disperse** **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt **Disperse** Max. Cons.
Capture of Shipment.	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**

Taken together these modes, human initiated event strategies, and hypothesized consequence outcomes can be conglomerated into a risk matrix for simplified use by risk managers, security personnel and for the specific purposes of risk identification, analysis and mitigation. A radioactive dispersal, whether it is considered minimum, moderate or catastrophic for the purposes of analysis, depends on many variables, including the age of the fuel, the burn-up history of that fuel, the crud inventory in the transport cask, the degradation of the cladding, the number of assemblies in a given cask, and so forth. However, a properly constructed assessment process can address these variables, and recommend appropriate countermeasures and mitigation strategies.

CONCLUSION

First and foremost, the materials in question, huge quantities of highly radioactive wastes from nuclear power plants and weapons production facilities, **do *not have to be transported*** across America to Yucca Mountain. The energy industry has assured the public that power plants are safe and secure, thus ***sheltering the wastes in place*** at these facilities seems the prudent thing to do. At these secure facilities they would not be subject to protests, labor unrest, sabotage or terrorism during transit activities, in short they are safer where they sit.

Likewise, if the program does move forward, alternatives to DOE management exist. As the NAS has suggested, DOE could be replaced as the agency of responsibility for the proposed Yucca Mountain project. This action would help the creditability of the proposal since many stakeholders and members of the general public have historic reasons to distrust this agency and its claims regarding safety and security. This is one option for you to consider in you oversight role.

If the program does proceed and DOE is left in charge, the last portion of the testimony examined the current state of risk assessment for human-initiated events against SNF and HLW shipments to the proposed repository at Yucca Mountain, Nevada. In the process this analysis identified a variety of potential human initiated event scenarios for consideration by this agency and its transportation planners. These represent a range of creditable threats, consequences and for a variety of transportation components that would be used during a transportation campaign.

The attack scenarios evaluated in the Draft Supplemental EIS for Yucca Mountain, and the Draft Nevada Rail Alignment EIS, repeat the methods used by DOE and NRC over the past three decades. They are not proactive in response to 9/11 and do not reflect state of the art risk assessment techniques. The DOE/NRC analyses assumed single-phase attack scenarios and other limiting assumptions that may artificially constrain the results. None of these consequence assessments have evaluated impact-exacerbating tactics, such as combined use of a breaching device and a dispersal device, or use of multiple breaching devices. None of these consequence assessments have evaluated the impact-exacerbating tactics studied by counter-terrorism experts in the post-9/11 environment. This testimony advocates use of an analysis-in-depth method that uses current risk assessment methods, but adds the well known AVA as an extra layer of protection to offset the change in the risk environment due to terrorism. The purpose of the AVA technique is to harness the creatively and ingenuity of people outside

an organization like the DOE and in doing so improve the risk analysis. Such an approach would respond to the WGA resolution on transportation terrorism risks.

Ways to Review DOE Efforts

In the post 9/11 world almost all federal agencies with a significant homeland security role have had to rethink their assumptions on how best to serve the public interest. One conclusion suggested from the alternative scholarship on Yucca Mountain transportation risks is that the DOE does not get it – they are stuck in an engineering based bureaucratic paradigm, or if you will, an organizationally dysfunctional way of thinking. This DOE mindset prevents this agency from looking outside of their narrowly defined transportation risk assessment agendas.

In the case of Yucca Mountain, the unwritten "demand" for programmatic progression after years of DOE management seemingly overrides a systematic and serious reconsideration of risks for the transportation of these radioactive materials. The need to reform the DOE's work on Yucca Mountain in light of the new threat environment is not evidenced by this agencies continued refusal to acknowledge real and pressing issues with their planning for shipments to Yucca Mountain.

The DOE is continually revising their transportation concept for Yucca Mountain and could readily alter their current program to adopt the recommended risk reduction process. Considering the currently delayed schedule for the repository and the proposed rail line, it seems unlikely that shipments to Yucca Mountain could begin earlier than 2017-2020. There is ample time for another agency or if left in charge, for the DOE, to systematically address human-initiated events. Revision of such documents as the various Supplemental EIS's, Transportation Concept of Operations, National Transportation Plan, national routing studies, and in its implementation of Section 180© technical and financial assistance to affected States and Indian Tribes would at a minimum be desirable.

If this testimony could leave this committee with only three points to consider, they would be:

Point One:

- Yucca Mountain transportation is risky and will present a target rich environment for adversaries. The shipments are symbolically important and represent a radiological significant target.

- The solution is to shelter the shipments in place at the sites of waste origin. As noted by the NRC, energy industry and others, they are safe and secure faculties. Why expose wastes to risks during transportation if not necessary?

Point Two:

- DOE has systematically neglected to address the laundry lists of concerns brought forth by stakeholders. These deliberate choices by the DOE increase the likelihood of attacks, the consequences of those attacks and the resultant social dislocations if these attacks succeed.

- The solution is to compel the DOE to engage in a meaningful national level NEPA process that addresses stakeholder concerns that have been documented over the decades of Yucca Mountain debates.

Point Three:

- DOE, in consultation with stakeholders, should engage in systematic risk assessment method of analysis. In particular, it should use the AVA process in conjunction with other methods to provide a more robust triangulated analysis.

- The solution here is to do it and will allow the DOE to avoid the potentially fatal fault of being reactive to threats and become more proactive in relationship to human initiated events.

I wish to thank the committee for allowing me to offer an alternative perspective on this important issue. If you have any questions I will be happy to answer them.

---

[1] My training at the University of Nevada, Las Vegas was in political sociology, deviance, and criminology.

[2] This educational center is funded by the Office of the Director of National Intelligence (ODNI) as part of a grant to seven CSU's in the southern California area. The CSUN IC-CEA assists students who are considering careers in the intelligence field.

[3] The term "human initiated event" comes from Ballard, J. D. (2002). "Asymmetrical Sabotage Tactics: Nuclear Facilities/Materials and Vulnerability Analysis." Publication available at www.numat.at.

[4] In particular past projects have included Robert J. Halstead, Fred Dilger, Hank Collins and Marvin Resnikoff. The testimony herein reflects the authors interactions with, and the decades of work, these colleagues have contributed to the debates over Yucca Mountain.

[5] See "Testimony" before the *United States Senate*, Committee on Energy and Natural Resources, One-Hundredth Seventh Congress regarding S. J. Res.34 Approving the Site at Yucca Mountain, Nevada, for the Development of a Repository for the Disposal of High-level Radioactive Waste and Spent Nuclear Fuel, Pursuant to the Nuclear Waste Policy Act of 1982. May 2002. Available at http://www.yuccamountain.org/leg/ballard052202.html. See also "Testimony of James David Ballard." *United States House of Representatives*, Subcommittee on Highways and the House Subcommittee on Transportation and Infrastructure. April 2002. Available at http://gopher.house.gov/transportation/highway/04-25-02/ballard.html.

[6] Nevada and other scholars have for many years discussed this idea in a variety of forums and forms. This section briefly summarizes that body of literature. For more complete details see: Nuclear Regulatory Commission Documentation for Petition." Agency petition for Rulemaking pursuant to 5 U.S.C. § 553 and 10 C.F.R. § 2.800 - 2.804. *Federal Register*. September 1999 and Halstead, R. J., F. Dilger and J. D. Ballard. (2005) "Planning for an Unpredictable Event: Response to Terrorist Attack against SNF Shipment." *Waste Management* conference proceedings. See also "Testimony" before the *United States Senate*, Committee on Energy and Natural Resources, One-Hundredth Seventh Congress regarding S. J. Res.34 Approving the Site at Yucca Mountain, Nevada, for the Development of a Repository for the Disposal of High-level Radioactive Waste and Spent Nuclear Fuel, Pursuant to the Nuclear Waste Policy Act of 1982. May 2002. Available at http://www.yuccamountain.org/leg/ballard052202.html and "Testimony of James David Ballard." *United States House of Representatives*, Subcommittee on Highways and the House Subcommittee on Transportation and Infrastructure. April 2002. Available at http://gopher.house.gov/transportation/highway/04-25-02/ballard.html for more specifics on symbolic attacks, target rich environments and associated issues.

[7] See Ballard, J. D. (2002). "Shelter-In-Place: The Logic of High-Level Nuclear Waste Security." Agency paper. State of Nevada's Agency for Nuclear Projects: Carson City, NV. Based on a presentation at Stanford University, January 2002.

[8] See Halstead, R. J., F. Dilger, J. D. Ballard and H. Collins (2008). "State of Nevada Perspective on the U.S. Department of Energy Yucca Mountain Transportation Program." Paper #8154. Waste Management Conference 2008 proceedings. Publisher: Waste Management, Phoenix, AZ.

[9] Nevada has publically communicated these recommendations to the DOE as well as the U.S. Nuclear Regulatory Commission (NRC), the NRC Advisory Committee on Nuclear Waste, the U.S. General Accounting Office (GAO), the U.S. Nuclear Waste Technical Review Board, the National Academy of Sciences (NAS) Study Committee on Transportation of Radioactive Waste, the National Association of Regulatory Utility Commissioners, and other agencies and organizations.

[10] Ballard, J. D., R. J. Halstead, F. Dilger, H. Collins and M. Resnikoff. (2008). "Assessing the Vulnerability of Yucca Mountain Shipments: A Threat Matrix for Human-Initiated Events." Paper #8152. Waste Management 2008 Conference proceedings. Publisher: Waste Management, Phoenix, AZ.

[11] The use of open source documents as the basis of this presentation and as the means to develop this methodology should demonstrate to the committee the level of publically available materials that potential adversaries can access. Specific attack details and details on tactics have deliberately been left out of this presentation in consideration of safety and security.

[12] See Halstead, R. J. and J. D. Ballard. (1997). "Nuclear Waste Transportation Security and Safety Issues: The Risk of Terrorism and Sabotage against Repository Shipments." Prepared for the state of Nevada, Agency for Nuclear Projects (October 1997; Revised, December 1998). This report can no longer be accessed on the web due to security concerns, but can be requested in writing from Mr. Joseph Strolin, Administrator, Agency for Nuclear Projects, Suite 118, 1761 E. College Parkway, Carson City, NV 89706. Also refer to J.D. Ballard, R.J. Halstead, F. Dilger, H. Collins, "Planning for an Unpredictable Event: Vulnerability and Consequence Reassessment of Attacks on Spent Fuel Shipments," revised version of a paper presented at Waste Management 2005. The revised paper was not included in the proceedings, but it is available on line at http://www.state.nv.us/nucwaste/trans.htm. Lastly, see *North Atlantic Treaty Organization* (NATO). Project # SST.CLG.978964, "Terrorism Attacks on Nuclear Power Plants and Nuclear Materials Transports." This large research group was led by Dr. Friedrich Steinhausler, Institute for International Security, Stanford University. October 2001 to July 2004. A final report was submitted to NATO but to date has note been released.

[13] The NRC and DOE continue to use the singular terminology of "sabotage" to designate any incident related to human initiated events. The use of the term human initiated events herein was originally coined to help move forward the discussions of risks to a more encompassing discussion in the post 9/11 threat environment.

[14]DOE. (1999). "Draft Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada," DOE/EIS-0250D, U.S. Department of Energy, Washington, DC (July 1999).

[15] LUNA, R. et al. (1999). "Projected Source Terms for Potential Sabotage Events Related to Spent Fuel Shipments," SAND99-0963.

[16] DOE. (2002). "Final Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada," DOE/EIS-0250. Available on the web at http://www.ymp/gov/documents/feis_a/index.htm.

[17] LAMB, M. et al. (2002). " Potential Consequences of a Successful Sabotage Attack on a Spent Fuel Shipping Container: An Analysis of the Yucca Mountain EIS Treatment of Sabotage." Prepared by Radioactive Waste Management Associates for the State of Nevada, Agency for Nuclear Projects.

[18] Respectively: DOE. (2007). "Draft Supplemental Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada" DOE/EIS-0250F-S1D and DOE, "Draft Supplemental Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada – Nevada Rail Transportation Corridor," DOE/EIS-0250F-S2D and "Draft Environmental Impact Statement for a Rail Alignment for the Construction and Operation of a Railroad in Nevada to a Geologic Repository at Yucca Mountain, Nye County, Nevada," DOE/EIS-0369D.

[19] LUNA, R, (2006). "Release Fractions from Multi-Element Spent Fuel Casks Resulting from HEDD Attack," Waste Management 2006 conference. Publisher: Waste Management, Phoenix, AZ.

[20] DOE. (2007). See page 6-21 from "Draft Supplemental Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada" DOE/EIS-0250F-S1D and DOE.

[21] See Ballard, J. D., R.J. Halstead, F. Dilger, H. Collins. (2007). "Yucca Mountain Transportation Security Issues: Overview and Update." Waste Management 2007 conference. Publisher: Waste Management, Phoenix.

[22] WGA. "Making the West the Best: Western Governors' Association 2007 Annual Report". Available online at: http://www.westgov.org/wga/publicat/annrpt07.pdf.
[23] WGA. "Western Governors Association Policy Resolution 07-02: Assessing the Risks of Terrorism and Sabotage against High-Level Nuclear Waste Shipments to a Geologic Repository or Interim Storage Facility."
[24] WGA. "Western Governors Association Policy Resolution 07-02: Assessing the Risks of Terrorism and Sabotage against High-Level Nuclear Waste Shipments to a Geologic Repository or Interim Storage Facility."
[25] Ballard, J. D. (2002). "Asymmetrical Sabotage Tactics: Nuclear Facilities/Materials and Vulnerability Analysis." Publication available at www.numat.at.
[26] See Ballard, J. D., R.J. Halstead, F. Dilger, H. Collins. (2007). "Yucca Mountain Transportation Security Issues: Overview and Update." Waste Management 2007 conference. Publisher: Waste Management, Phoenix. Also Ballard, J. D. (2002). "Asymmetrical Sabotage Tactics: Nuclear Facilities/Materials and Vulnerability Analysis." Publication available at www.numat.at.
[27] DOE. (2006). "Transportation System Concept of Operations," DOE/RW-0584 and DOE. (2007). "National Transportation Plan," pre-decisional draft dated July 16, 2007.
[28] Ballard, J. D. (2002). "Asymmetrical Sabotage Tactics: Nuclear Facilities/Materials and Vulnerability Analysis." Publication available at www.numat.at.
[29] MARENKO, T. (2007). "Terrorist Threat to Energy Infrastructure Increases," *Jane's Intelligence Review*, Download date July 28, 2007. Available online at http://www.ciaonet.org/wps/mat04/mat04.pdf.
[30] See Halstead, R. J. and J. D. Ballard. (1997). "Nuclear Waste Transportation Security and Safety Issues: The Risk of Terrorism and Sabotage Against Repository Shipments." Prepared for the state of Nevada, Agency for Nuclear Projects (October 1997; Revised, December 1998). Ballard, J. D., R. J. Halstead, F. Dilger, H. Collins and M. Resnikoff. (2008). "Assessing the Vulnerability of Yucca Mountain Shipments: A Threat Matrix for Human-Initiated Events." Paper #8152. Waste Management 2008 Conference proceedings. Publisher: Waste Management, Phoenix, AZ. J.D. Ballard, R.J. Halstead, F. Dilger, H. Collins, "Planning for an Unpredictable Event: Vulnerability and Consequence Reassessment of Attacks on Spent Fuel Shipments," revised version of a paper presented at Waste Management 2005. Ballard, J. D. (2002). "Asymmetrical Sabotage Tactics: Nuclear Facilities/Materials and Vulnerability Analysis." Publication available at www.numat.at. CRS. (2007). "Nuclear Power Plants: Vulnerability to Terrorist Attack." RS 21131. NAS. (2006). "Going the Distance? The Safe Transport of Spent Nuclear Fuel and High-Level Radioactive Waste in the United States." Washington, DC: The National Academies Press). R.J. Halstead, F. Dilger, J.D. Ballard. (2004). "Beyond the Mountains: Nuclear Waste Transportation and the Rediscovery of Nevada." Waste Management 2004 Conference, February 25 – March 1, 2004, Tucson, AZ.
[31] See Johnson, R.G. (2004). "Adversarial Safety Analysis: Borrowing the Methods of Security Vulnerability Assessments," Journal of Safety Research 35: 244-248 and Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[32] Broder, J.F. (1999). *Risk Analysis and the Security Survey*. Boston: Butterworth-Heinemann.
[33] Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[34] Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[35] See Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt; Kumamoto, H., E.J. Henley. (2000). *Probabilistic Risk Assessment and Management for Engineers and Scientists.* Hoboken, NJ: Wiley; Roper, C. (1999). *Risk Management for Security Professionals.* Boston: Butterworth-Heinemann; KNIEF, R. (1991). *Risk Management: Expanding the Horizons in Nuclear Power and Other Industries*, Boca Raton, FL: CRC Press; Starr, C. "Risk Management, Assessment, and Acceptability." *Risk Analysis*, Volume 5 (1985).
[36] Hamalainen, R.P., M.R.K. Lindstedt, and K. Sinkko. (2000). *Multiattribute Risk Analysis in Nuclear Emergency Management.* Malden, MA: Blackwell Publishing; Rayner, S. and R. Cantor. (1987). "How Fair is Safe Enough.: The Cultural Approach to Societal Technological Choice." *Risk Analysis*, Volume 7.
[37] Pidgeon, N., R.E. Kasperson, and P. Slovic. (2003). *The Social Amplification of Risk.* New York: Cambridge University Press; Slovic, P. (1993). "Perceived Risk, Trust, and Democracy." *Risk Analysis*, Volume 13.

[38] Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt; Willis, H. H., A. R. Morral, T. K. Kelly and J.J. Medby. (2005). *Estimating Terrorism Risk*. Santa Monica: Rand Corporation (2005).
[39] Clarke, L. (2001). Mission *Improbable: Using Fantasy Documents to Tame Disaster*. Chicago, Illinois: University Of Chicago Press.
[40] NRC. "Design Basis Threat." Download date August 5, 2007. Available online at http://www.nrc.gov/; Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[41] NRC. "Design Basis Threat." Download date August 5, 2007. Available online at http://www.nrc.gov/; Blankenship, J. (2005). "International Standard for Design Basis Threat (DBT)." Paper presented at the NUMAT Conference, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/; Chetvergov, S. (2005). "Evolution of Nuclear Security in the Republic of Kazakhstan." Paper presented at NUMAT Conference, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/; Ellis, D. (2005). "Training Programs for the Systems Approach to Nuclear Security." Paper presented at NUMAT Conference, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/.
[42] NRC. "Design Basis Threat." Download date August 5, 2007. Available online at http://www.nrc.gov/; Khripunov, I. (2005). "Nuclear Security Culture: A Generic Model for Universal Application." Paper presented at NUMAT Conference, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/.
[43]Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[44] Blankenship, J. (2005). "International Standard for Design Basis Threat (DBT)." Paper presented at the NUMAT Conference, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/
[45]IAEA. (2007)., "Requirements for Physical Protection Against Sabotage of Nuclear Facilities and Nuclear Material During Use and Storage." Download date: August 5, 2007. Available online at http://www.iaea.org/; NRC. (2005). "Design Basis Threat," *Federal Register*, Volume 70, Number 214; Hirsch, D., D. Lochbaum, and E. Lyman, "The NRC's Dirty Little Secret: The Nuclear Regulatory Commission is Still Unwilling to Respond to Serious Security Problems." *Bulletin of Atomic Scientists*, Volume 59 (May-June 2003); GAO. (July 26, 2005). "Nuclear Security: Actions Needed by DOE to Improve Security of Weapons-Grade Nuclear Material at its Energy, Science and Environmental Sites: Statement of Gene Aloise, Director, Natural Resources and Environment." Testimony before the Subcommittee on National Security, Emerging Threats and International Relations, United States House of Representatives; GAO. (April 4, 2006)., "Nuclear Power: Plants Have Upgraded Security, but the Nuclear Regulatory Commission Needs to Improve its Process for Revising the Design Basis Threat: Statement of Jim Wells, Director: Natural Resources and Environment." Testimony before the Subcommittee on National Security, Emerging Threats and International Relations, United States House of Representatives.
[46] Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[47] S. Kondratov, F. Steinhausler. (2005). "Why there is a need to Revise the Design Basis Threat Concept." Paper presented at NUMAT Conference, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/
[48] GAO. (July 26, 2005). "Nuclear Security: Actions Needed by DOE to Improve Security of Weapons-Grade Nuclear Material at its Energy, Science and Environmental Sites: Statement of Gene Aloise, Director, Natural Resources and Environment." Testimony before the Subcommittee on National Security, Emerging Threats and International Relations, United States House of Representatives; GAO. (April 4, 2006)., "Nuclear Power: Plants Have Upgraded Security, but the Nuclear Regulatory Commission Needs to Improve its Process for Revising the Design Basis Threat: Statement of Jim Wells, Director: Natural Resources and Environment." Testimony before the Subcommittee on National Security, Emerging Threats and International Relations, United States House of Representatives.
[49] Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.

[50] Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[51] E.G. Bitzer, and R. Johnson. (2007). "Creative Adversarial Vulnerability Assessments," *Journal of Physical Security*, Volume 2. Download date: August 7, 2007. Available on-line at http://jps.lanl.gov/.
[52] Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[53] Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[54] Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[55] Lubenau, J. O. and D. J. Storm. (2002). "Safety and Security of Radiation Sources in the Aftermath of 11, September 2001." *Health Physics* 83: 155-164 (2002).
[56] Moore, D. A., B. Fuller, M. Hazzan, and J. W. Jones. (2007). "Development of a Security Vulnerability Assessment Process for the RAMCAP Chemical Sector," *Journal of Hazardous Materials* 142: 689-694.
[57] See Johnson, R.G. (2004). "Adversarial Safety Analysis: Borrowing the Methods of Security Vulnerability Assessments," Journal of Safety Research 35: 244-248 and Johnson, R.G. (2005). "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL. Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt.
[58] Busenberg, G. J. (1999). "Collaborative and Adversarial Analysis in Environmental Policy," *Policy Sciences* 32. Download date: August 8, 2007. Available on-line at: www.springerlink.com.
[59] Bettie, J. (2007). "NRC Takes Two Roads on Terror Review Issue." *The Energy Daily*, February 27, 2007.